Docket No. 3037-4196

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No.: 09/630,711
Confirmation No.: 7518

Applicants: B.M. JAKOBSSON *et al.*
Group Art Unit: 2131
Examiner: Aravind K. Moorthy

Filed: August 1, 2000

Customer No.: 27123

For: PROOFS OF WORK AND BREAD PUDDING PROTOCOLS

DECLARATION UNDER 37 C.F.R.§ 1.132

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

1. I, Ganapathy S. Sundaram, declare and state that:

2. I am a citizen of INDIA;

3. I am a co-author of published papers relating to cryptography, a partial list of which is as follows:

   a) "An efficient discrete log pseudorandom generator", Advances in Cryptology, CRYPTO '98, Santa Barbara, USA.

   b) "Towards making Luby-Rackoff ciphers practical and optimal", Fast software encryption workshop, Rome 1999.

   c) "Luby-Rackoff ciphers over finite algebraic structures OR Why XOR is not so exclusive?", Selected Areas in Cryptography, SAC 2002.

   d) "Efficient constructions of variable input length block ciphers", Selected areas in cryptography, Selected Areas in Cryptography, SAC 2004.

4. I am an inventor or co-inventor of patents related to cryptology and related technologies, as follows:

   a) USP 6,285, 761, Issued September 4, 2001, Patel 3-1 USA, entitled "A Method for Generating Pseudo-Random Numbers";

   b) USP 6,502,062, Issued December 31, 2002, Acharya 9-16-4 USA, entitled, "A System and Method for Scheduling Data Delivery Using Flow and Stretch Algorithms";

   c) USP 6,836,666, Issued December 28, 2004, Gopalakrishnan 9-7-19-9 USA, entitled "Method to Control Uplink Transmission in a Wireless Communication System";

   d) USP 6,859,446, Issued February 22, 2005, Gopalakrishnan 3-2-5-2-14-1-7-13 USA, entitled "Integrating Power-Controlled and Rate-Controlled Transmission on a Same Frequency Carrier";

   e) USP 6,930,981, Issued August 16, 2005, Gopalakrishnan 7-6-10-57-7-8, entitled "Method for Data Rate Selection in a Wireless Communication System";

   f) USP 7,058,946, Issued June 6, 2006, Acharya 18-18-18 USA, entitled "Adaptive Scheduling of Data Delivery in a Central Server";

   g) USP 7,092,731, Issued August 15, 2006, Gopalakrishnan 18-5-16 USA, entitled "Method for Improviing Capacity of a Reverse Link Channel in a Wireless Network";

   h) USP 7,110,466, Issued September 19, 2006, Gopalakrishnan 2-11-6 USA, entitled "Variable Rate Message Coding";

   i) USP 7,117,424, Issued October 3, 2006, SUndaram 12-1 USA, entitled "Block Coding Method Having Increased Flexibility in Choice of Code Length or Minimum Code Distance";

   j) USP 7,158,504, Issued January 2, 2007, Kadaba 8-14-15-20-11-2-1 USA, entitled "Multiple Mode Data Communication System and Method and Forward and/or Reverse Link Control Channel Structure"; and

   k) USP 7,221,756, Issued May 22, 2007, Patel 17-3-10 USA, entitled "Constructions of Variable Input Length Cryptographic Primitives for High Efficiency and High Security".

5. I hold academic degrees and honors, as follows:

   a) PhD in Mathematics, specializing in Algebraic Geometry from Purdue University, West Lafayette, Indiana, granted in 1997;

   b) Distinguished Member of the Technical Staff at Bell Laboratories, Lucent Technologies (now Alcatel-Lucent) from September 2000 to present date.

6. I have experience in cryptology through employment with Lucent Technologies (now Alcatel-Lucent) – June 1997 – To date.

7. I have read and understood the disclosed technical subject matter and the claimed subject matter in the above - indicated US Patent Application Serial Number 09/630,711.

8. I state that, contrary to the Examiner's Advisory Action of June 4, 2007 for the above-identified application, (1) the terms "certain amount", "intense" and "useful computation" are clearly disclosed and described in the subject application to those skilled in the cryptography art, which includes "Proof of Work", and (2) that one skilled in the art would be able to implement and use the claimed subject matter using the disclosure as a guide, based on the technical subject matter described in the specification, as follows:

   a) The term "certain amount of intense computation "is described by the Definitions 1-4 at page 6 in the above-identified application. The Definitions define and measure a certain amount of intense computation for a Proof of Work (POW) by (a) steps of the computation (w); (b) amount of memory (m) available for the computation, and (c) the time interval (ts, tc) for the computation. As a worker skilled in the cryptology art, I state that the parameters w, m and (ts,tc) are pre-specified and unambiguous and describe and measure a "certain amount of intense computation". The intensity of the computation for a POW is further understood from the number of computation steps (w) needed to be performed and a security parameter (l), which is well understood to be of the order of 2^{80} or 2^{100}.

   b) The term "useful computation" is understood from the description of an Entity compiling replies from other entities into a single POW for a Verifier. A worker skilled in the art would know that the Entity would need to perform calculations to merge the different replies from the various Entities into single POW for a useful operation, i.e. the verification of the POW by a Verifier, described in Figure 3, steps 330 and 335 of the above-identified application.

9. I hereby declare that all statements made herein of my own knowledge are to the best of my knowledge true and that all statements made on information and belief are to the best of my knowledge believed to be true; and further that these statements were made with the knowledge that willful false statements are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the subject application or any patent issuing thereon.

Date: August 03, 2007 By: Ganapathy